REPORT DOCUMENTATION PAGE

AFRL-SR-BL-TR-01-

0484

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REI
		01 Jun 97 to 31 May 01 Final

4. TITLE AND SUBTITLE
(AASERT-95) (BMDO) Quantum and Classical Cryptograph for Security and Privacy in Photonic Networks

5. FUNDING NUMBERS
61103D
3484/TS

6. AUTHOR(S)
Professor Fainmna

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0934

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFOSR/NE
801 North Randolph Street Rm 732
Arlington, VA 22203-1977

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
F49620-97-1-0389

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
APPROVAL FOR PUBLIC RELEASED; DISTRIBUTION UNLIMITED

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

We have developed rigorous definitions and mathematical formalism for information leakage through possible eavesdropping on th quantum channel. We have investigated classical cryptograph using nonlinear optical processor based on three-wave and four-wave mixing in nonlinear crystals. The processors operate with femtosecond response time and unlike commonly used autocorrelators, allows time-to-space conversion of both amplitude and phase information carried by ultrashort pulses. Pulse position modulation is combined with CDMA techniques to allow enhanced privacy optical networking with ultrahigh bandwidth utilization.

14. SUBJECT TERMS			15. NUMBER OF PAGES
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Final Technical Report

for AASERT

Quantum and Classical Cryptography for Security and Privacy of Photonic Networks.

Sponsored by

Air Force Office of Scientific Research

Ballistic Missle Defence Organization

Under Grant F-49620-97-1-0389

for Period 06/01/97 through 05/31/01

Grantee

The Regents Of the University of California, San Diego

University of California , San Diego

La Jolla CA 92093

Principal Investigators: Y. Fainman

(619) 534-8909 (619) 534-7919

Program Manager: Dr. Gernot Pomrenke and Dr. Alan Craig

703-696-8426

2. Objectives/Statement of work

A. Investigate quantum cryptography protocols and realizations with frequency division techniques.

B. Study classical cryptography and realization with ultra-short laser pulses and space-time spectral-domain nonlinear optical processing.

3. Status of effort

A. We have developed rigorous definitions and mathematical formalism for information leakage through possible eavesdropping on the quantum channel.

B. We have investigated classical cryptography using nonlinear optical processor based on three-wave and four-wave mixing in nonlinear crystals. The processors operate with femtosecond response time and, unlike commonly used autocorrelators, allows time-to-space conversion of both amplitude and phase information carried by ultrashort pulses. Pulse position modulation is combined with CDMA techniques to allow enhanced privacy optical networking with ultrahigh bandwidth utilization.

4. Accomplishments/New Findings

In the following we briefly summarize the accomplishments in the focus areas being investigated under the AASERT project: (A) Quantum Cryptography and (B) Classical Cryptography using CDMA methods.

A. Security of quantum cryptography in a noisy environment

We continued investigating the quantum cryptography research that was initiated by the FRI program on the relationship between the induced error rate and the maximum amount of information the eavesdropper can extract, both in the two-state B92 and the four-state BB84 quantum cryptographic protocols. Analysis was limited to eavesdropping strategies where each bit of the quantum transmission is attacked individually and independently from other bits. Subject to this restriction, however, we believe all attacks not forbidden by physical laws are taken into account. For both B92 and BB84, we are explicitly constructing the optimal eavesdropping method that on average yields the most information for a given error rate. In each case, a closed-form functional dependence between the error rate and the information yield is investigated.

Additionally, we continued investigating the bisect-and-discard error-correction protocol relying on disclosing the parity of blocks of bits and discarding bits so that the errors are corrected. The task is using the bisection and parity disclosure procedure proposed to remove the K errors. The string of N bits is first divided into blocks of p bits whose parity is checked: in case of parity mismatch the block is divided into two halves and the parity is again checked-this bisection and parity check proceeds until the block are only two bits long. In case of a parity match, one bit is discarded and the parity of the next block is examined. We derive the analytic expression for the bound on the probability that j-bit are in error. The crucial hypothesis in the derivation of the analytical expression was that we can calculate the average in the next iteration using the average of the previous one. To test this hypothesis, we have written a Monte Carlo simulation of the error correction procedure. Other protocols, most notably using pre-determined block sizes based on estimate of the error rate in every iteration are being implemented. In the following we briefly summarize our findings.

A. 1. Protocols for Secure Quantum Communication

A realistic quantum information system must function in the presence of noise and channel loss inevitable in any practical transmission. To guarantee full security of the transmission, it becomes necessary to assume that all observed errors are eavesdrop-induced. Nevertheless, a secure key can be distilled by means of a post-transmission negotiation over an open channel, albeit at a much reduced rate. We have examined the effects of channel limitations on the secrecy capacity of the BB84 protocol.

The sequence of steps in key distillation is illustrated in Fig. 1. Starting from m bits of *raw data*, Alice and Bob first discard any inconclusive bits and arrive at the n–bit sifted data. Next, they reconcile data using an error correction technique similar to the Cascade protocol. The value of an error bit identified by Cascade is always revealed to the eavesdropper through the block parities made public while locating it. Alice and Bob therefore discard the e_T bits found to be in error, and keep the remaining $(n-e_T)$–bit *corrected data.*

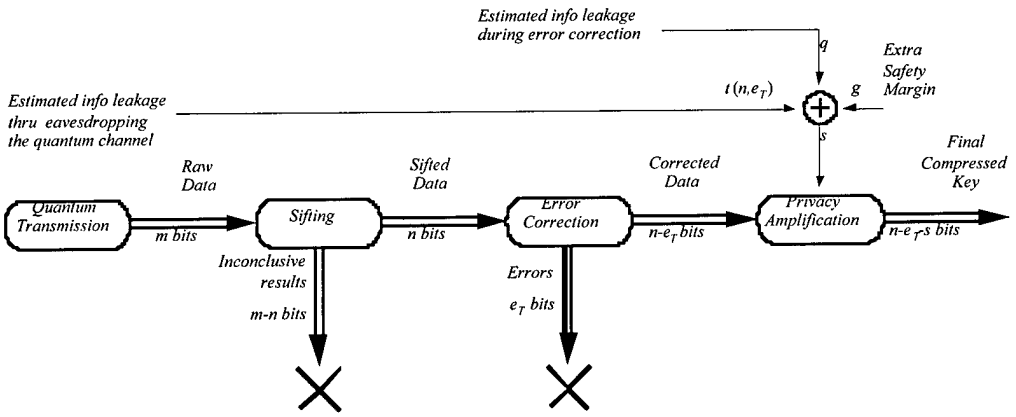

Fig. 1. The key distillation sequence.

In the next and most important step, the adversary's knowledge of the corrected data is assessed. Alice and Bob make an upper bound estimate $t(n,e_T)$ of Eve's Renyi information of order 2 with respect to the $(n-e_T)$–bit corrected data at the end of the quantum transmission. As the notation implies, the estimate $t(n,e_T)$ is determined from the size of the sifted data n and number of errors e_T. (The number of inconclusive results $m-n$ could also play a role in the decision, but the particular key distillation scheme presented here does not take it into consideration.) We call $t(n,e_T)$ the *defense function* because it is chosen by Alice and Bob to defend against an eavesdropping attack. Without loss of generality the defense function is agreed in advance of the transmission.

More accurate assessment of information leakage and error correction costs leads to a better estimate of secrecy capacity. Leakage estimates are also important in their own right, because Alice and Bob must use them during key distillation as explained previously. These estimates, and related issues, are the subject of our work.

One set of problems is posed by information leakage through possible eavesdropping on the quantum channel. We have developed for the first time the rigorous definitions and the mathematical formalism for making such estimates. According to our scheme, Alice and Bob analyze each of the anticipated eavesdropping strategies for its intrusiveness (the error rate likely to result from it), and its yield (the amount of information an eavesdropper is likely to gain). Such an analysis, which is based on the joint probability distribution of Bob's and Eve's outcomes, requires a quantum mechanical definition of the strategy. This description however,

can remain quite generic. The task is easily accomplished, for example, with respect to any strategy yet described in the literature. We demonstrate how intrusiveness and yield measures lead to a *defense function* for a given strategy. Alice and Bob's adopted estimate of information leakage through eavesdropping $t(n,e_T)$, which we call the *defense frontier*, is a function of their observed error rate such that it lies above and to the left of the defense functions constructed for all anticipated eavesdropping strategies (Fig. 2). As shown in Fig.1, the defense frontier must be taken into consideration by Alice and Bob when deciding the amount of compression necessary to protect their key, which in turn affects secrecy capacity of the system.

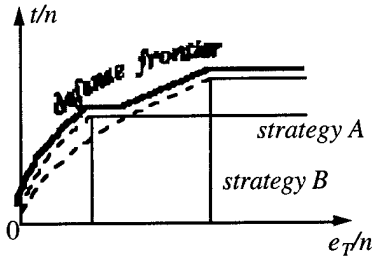

Fig. 2. Defense Frontier $t(n,e_T)$.

Finally, privacy amplification is applied to extract a shorter but unconditionally secure $(n-e_T-s)$–bit key from the corrected data. The number of bits s sacrificed at the privacy amplification stage depends on $t(n,e_T)$, the amount q of additional Renyi information leaked to Eve during error correction, and on the safety margin g determined by Alice's and Bob's security requirements. Provided that the estimate $t(n,e_T)$ holds (i.e., that Eve's actual information on the corrected data $I_T^R \le t(n,e_T)$), the final key is almost perfectly secret from Eve except with a small probability. The key distillation framework permits Alice and Bob to ensure that, except with an arbitrarily small probability, the attacker (if any) can possess no more than an arbitrarily small amount of information on their final key. Although the security of the key is never absolute, it can be increased exponentially if the parties are prepared to reduce the size of the key. Furthermore, the security does not rest on any assumptions limiting the enemy's computational power. Alice and Bob thus obtain what in the parlance of classical cryptography is known as an unconditionally secure key. Quantum cryptography, however, remains a young field of study, with many questions still unanswered. Some of these unanswered questions will need to be further investigated.

A. 2 Information leakage through eavesdropping

While our derivations cover a very general class of eavesdropping attacks, it is nonetheless subject to important limitations. First, the discussion assumed that the carrier states $|\mathbf{u}\rangle,|\mathbf{v}\rangle,|\bar{\mathbf{u}}\rangle,|\bar{\mathbf{v}}\rangle$ transmitted by Alice are pure states in the same Hilbert plane H, and that Bob makes his von Neumann measurements in H. These ideal conditions can be satisfied only approximately in practice. All physically prepared states are, strictly speaking, mixed states, and even if they were pure, no three states would precisely belong to the same plane. Although secure quantum communication is possible with a slightly defective source, it is necessary to ascertain how much additional information may be leaked to the eavesdropper because of the defect.

Suppose, for example, that in a BB84 protocol Alice emits a state $|\mathbf{v}'\rangle = \cos\gamma|\mathbf{v}\rangle + \sin\gamma|\mathbf{z}\rangle$ instead of $|\mathbf{v}\rangle$, where $|\mathbf{z}\rangle$ is normal to H, and Bob still measures incoming particles in the bases $\mathbf{B}_u = \{|\mathbf{u}\rangle,|\bar{\mathbf{u}}\rangle\}$, $\mathbf{B}_v = \{|\mathbf{v}\rangle,|\bar{\mathbf{v}}\rangle\}$ .One would then expect Eve to apply the measurement defined by

the orthogonal resolution of the identity $\{\mathbf{P}_z \triangleq |\mathbf{z}\rangle\langle\mathbf{z}|; \mathbf{P}_{uv} \triangleq |\mathbf{u}\rangle\langle\mathbf{u}| + |\mathbf{v}\rangle\langle\mathbf{v}|\}$. When Eve obtains the outcome **uv**, the input state is projected on H , and is not altered in any way that is detectable by Bob's receiver. When Eve obtains **z**, she retransmits a replica of $|\mathbf{v}'\rangle$ which she knows to have been the input state. The above strategy thus reveals to Eve a $\frac{1}{4}\sin^2\gamma$ fraction of all bits without inducing a single error. While the quantity $\frac{1}{4}\sin^2\gamma$ may be small in a particular transmitter, there is no obvious reason to believe that even stronger attacks taking advantage of the out-of-plane state vector components are not possible. More generally, no formal treatment has yet been offered in the literature of the vulnerabilities that may obtain when quantum cryptographic transmitters or receivers deviate from their idealized specifications. With respect to mixed states, the only known result is the condition for error-free eavesdropping on two mixed states.

Even if a data carrying particle were to leave Alice in a pure state that belongs to the plane H, it may not remain in H after interacting with Eve's probe. Consider B92 eavesdropping strategy where Eve intercepts each passing particle and measures it in the manner the protocol prescribes for Bob, i.e., in one of the bases $\mathbf{B}_u = \{|\mathbf{u}\rangle, |\bar{\mathbf{u}}\rangle\}$, $\mathbf{B}_v = \{|\mathbf{v}\rangle, |\bar{\mathbf{v}}\rangle\}$. When Eve obtains a conclusive result, she learns the data bit for certain and retransmits an exact copy; and when Eve's result is inconclusive, she blocks the particle so Bob receives nothing. Ultimately, the entire communication is error-free, and Eve has complete knowledge of it — a result a complacent Alice and Bob might have thought impossible. Here, the fact that Eve constructs a particle state (namely, the vacuum state) that does not lie in the plane H defeats the security theorem. Note that BB84 is apparently safe against the above attack, because in that case Eve cannot immediately tell whether her measurement of the intercepted particle has been successful. One possibility is for Bob to treat every non-detection as an error, but this is usually impractical because of the "natural" losses in the channel. In an alternative approach , Alice transmits instead of $|\mathbf{u}\rangle$ and $|\mathbf{v}\rangle$ the states

$$|\mathbf{u}'\rangle \triangleq \beta|\mathbf{b}\rangle + \tfrac{1}{2}(|\mathbf{u}\rangle - |\mathbf{v}\rangle), \qquad |\mathbf{v}'\rangle \triangleq \beta|\mathbf{b}\rangle - \tfrac{1}{2}(|\mathbf{u}\rangle - |\mathbf{v}\rangle), \tag{1}$$

where $\beta \triangleq \sqrt{\frac{1}{2}\left(1 + |\langle\mathbf{u}|\mathbf{v}\rangle|\right)}$ is a normalization constant, and $|\mathbf{b}\rangle$ is a *multi-particle* state (such as a bright coherent pulse) that upon attenuation becomes $\frac{1}{2}\beta^{-1}(|\mathbf{u}\rangle + |\mathbf{v}\rangle)$. Bob's receiver is designed to tap off the majority of the $|\mathbf{b}\rangle$ component from the incoming signal into an auxiliary detector, while leaving the orthogonal $(|\mathbf{u}\rangle - |\mathbf{v}\rangle)$ component undisturbed. Behind the tap, $|\mathbf{b}\rangle$ is attenuated into $\frac{1}{2}\beta^{-1}(|\mathbf{u}\rangle + |\mathbf{v}\rangle)$. This reduces the states $|\mathbf{u}'\rangle, |\mathbf{v}'\rangle$ in Eq. (1) to $|\mathbf{u}\rangle, |\mathbf{v}\rangle$, which are then measured as usual per the B92 specification. An attempt by Eve to block the signal altogether would now be noticed because the detector would fail to fire, whereas if Eve transmits only the $|\mathbf{b}\rangle$ part of the signal bit errors would occur between Alice and Bob. Observe, however, that the introduction of a beamsplitter complicates Bob's measurement beyond the two-dimensional von Neumann model considered in the past. No formal security analysis has been offered for this modification of the B92 protocol yet.

Furthermore, in relating the eavesdropper's information to the disturbance inflicted on the carrier states, the bit error rate need not be sole disturbance measure. Any other quantity available to Alice and Bob, for example, the rate of inconclusive outcomes, can serve the same purpose, so long as firm connection is demonstrated between deviation of this quantity from its interference-free level and the information acquired by the enemy. Indeed, several alternative metrics of disturbance have already been investigated, but their tampering detection power in the context of quantum cryptography is yet to be explored. It seems likely that the use of additional indicators, along with the error rate, would make the eavesdropper's task more difficult, and hence improve system throughput by allowing Alice and Bob to secure the transmission at the cost of sacrificing less data. Expected values for many such indicators can be constructed as an

additional constraint in optimizing information gain on Eve's behalf. Effectiveness of the various disturbance metrics and their combinations as estimators of information gain must remain a subject for proposed investigation.

A. 3 Information leakage due to error-correction

We also investigated the error correction step of the key distillation procedure illustrated in Fig.1. This step produces for the communicating parties a data string that is virtually error-free, and which in the final stage of the protocol can be compressed using non-linear hash functions, so that the eavesdropper information is reduced to an arbitrarily low level. Although noteworthy theoretical analysis has been done with respect to the compression phase, very little work has been done on the error-correction phase.

Considering that the quantum crypto-transmission has yielded a string of N raw bits shared between Alice and Bob, we assume further that some of the bits were publicly disclosed in order to estimate the error rate and the error rate was found to be $r=N/K$ meaning that it was estimated that there were K errors among those N bits. The task is using the bisection and parity disclosure procedure proposed to remove the K errors. The string of bits is first divided into blocks of p bits whose parity is checked: in case of parity mismatch the block is divided into two halves and the parity is again checked-this bisection and parity check proceeds until the block are only two bits long. In case of a parity match, one bit is discarded and the parity of the next block is examined.

We derive the analytic expression for the bound on the probability that j-bit are in error. The crucial hypothesis in the derivation of the analytical expression was that we can calculate the average in the next iteration using the average of the previous one. To test this hypothesis, we have written a Monte Carlo simulation of the error correction procedure. Given the number of raw bits N and the estimated number of errors K, we first generate K random numbers uniformly distributed over the string of bits. The block size is chosen to be $p=N/K$ and the parity check and discarding of bits is simulated for every block of the string. At the end both, the number of corrected errors and the number of discarded bits are computed and the new values of N and K are calculated. The simulation then generates new random numbers representing the errors and bisection is again commenced until all the errors have been removed.

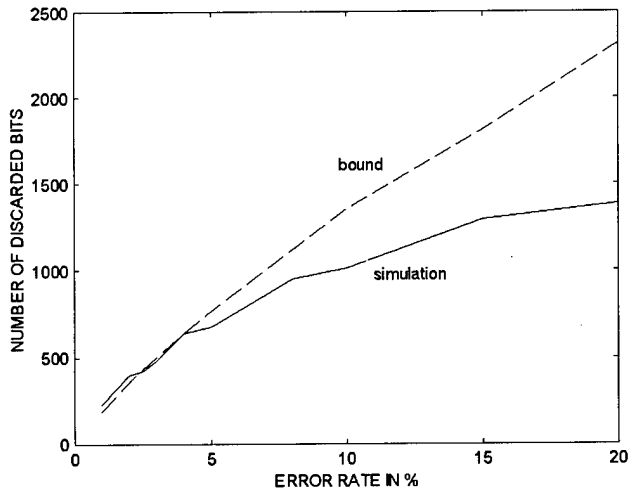

Figure 3. The cost of performing the error correction (in number of discarded bits) as a function of the error rate, 2000 raw bits were transmitted: full line - simulation; dashed line - the analytical expression.

Figure 3 gives a comparison between the simulations and the analytical expression curve in terms of the cost of performing the error correction (represented by the number of discarded bits necessary to remove the errors) versus the error rate. For fair comparison and in order to obtain average quantities, the simulation was run for 1000 transmissions and the average number of discarded bits was computed. The results are represented with full line for the simulation results and dashed line for the analytical expression. The agreement between the two results is very good for small error rates. For large error rates the analytic prediction gives increasingly poor results due to inaccuracy of the approximation $p_i = 2p_{i-1}$. Note that above 15% error rate out prediction indicates that all the bits should be sacrificed for performing the error correction (originally 2000 raw bits were established). Other protocols, most notably using pre-determined block sizes based on estimate of the error rate in every iteration are being implemented.

A. 4 Experimental quantum communication system

Our experimental work concentrated on a frequency division multiplexed (FDM) long distance interferometry (LDI) implementation of quantum cryptography. The FDM scheme is suitable for use in an optical fiber, because information is encoded on the phase difference between the signals at two closely spaced optical frequencies, which is expected to transmit reliably through a fiber without being significantly affected by environmental factors. We have investigated this assumption experimentally by subjecting a fiber to controlled temperature stress in the laboratory. We also assembled a prototype FDM LDI on an optical table from standard components, including photomultiplier tubes for single photon detection.

B. Classical Cryptography

Under the FRI program we have developed and experimentally demonstrated an all-optical post-processor that implements time-to-space demultiplexing and space-to-time multiplexing at femtosecond rates by exploiting spectral domain nonlinear three-wave mixing. For the studies of classical cryptography we have initiated investigation of time spreading methods using coherent detection techniques. This technoque uses spectral domain coding/decoding combined with our nonlinear spectral processor that allows time sequence imaging. The new technique is being analysed analitically and experimentally. The phase codes have been designed and fabricated for experimental evaluation and characterization of this novel technique.

B. 1 Privacy enhanced communication with CDMA coding

Ultrashort laser pulse technology has recently experienced significant advances, producing high peak power pulses of optical radiation a few femtoseconds in duration, corresponding to only a few cycles of its fundamental frequency. The unique properties of ultrashort laser pulses are ideally suited for various science and engineering applications including optical communications, medical and biomedical imaging, chemistry and physics. A common requirement of these applications is the ability to control the shape of the ultrashort pulses as well as to detect the shape of the pulses. Additionally, it becomes increasingly critical to create optical sources with ultra-broad spectral bandwidth to further utilize the available bandwidth (over 40Tbit/sec) of optical fiber networks. Ultrashort laser pulses may enable full, efficient utilization of the bandwidth of an optical network. Currently installed optical fibers serve as a low-loss point-to-point connections between electronic devices. While state-of-the-art electronic devices and systems may reach bit rates on the order of 10-100 Gbit/sec, a passive optical fiber has the potential to transmit bandwidths in excess of 10's of Tbit/sec. The 2-3 order-of-magnitude mismatch between optical fiber and electronic device capacities provides the design space to be utilized by novel processes. Possible approaches to increase the bit rate capacity of transmission systems include WDM employing CW laser sources, as well as time-division multiplexing (TDM) and CDMA based on ultrashort pulses.

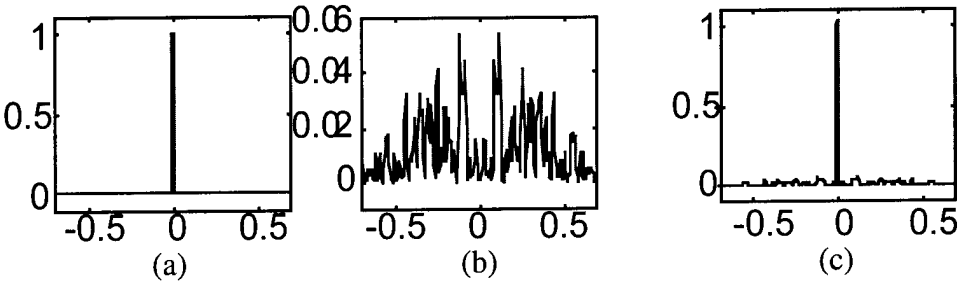

Fig. 4. (a) Input short pulse form. (b) Encoded signal, with increased duration and noise burst properties. (c) Received signal in a network environment, after decoding the transmitted pulse. Other users' signals appear as background noise.

Techniques of high resolution waveform synthesis by spectral filtering of ulrtashort laser pulses (ULP) in an optical processor have been developed, advancing the science of ultrafast phenomena. By employing a code-division-multiple-access (CDMA) as a spectral filter, the resulting optical waveforms can be used as a basis for a multiuser communication system with a spread time property. In the ULP-CDMA format, each user has a unique phase code from the orthogonal set for encoding a pulse before transmission on a common optical fiber carrier in an on-off-keying (OOK) modulation format. The desired signal is restored to a short pulse form (i.e., despread) at the receiver by applying a spectral filter consisting of the phase-conjugated code used at the transmitter-of-interest (see Fig. 4). The optical waveforms from other users remain as encoded pulses with long duration and low intensity. The decoded signal needs to be detected by a non-linear thresholding operation, as the temporal variation of the signal is too fast for direct electronic detection schemes.

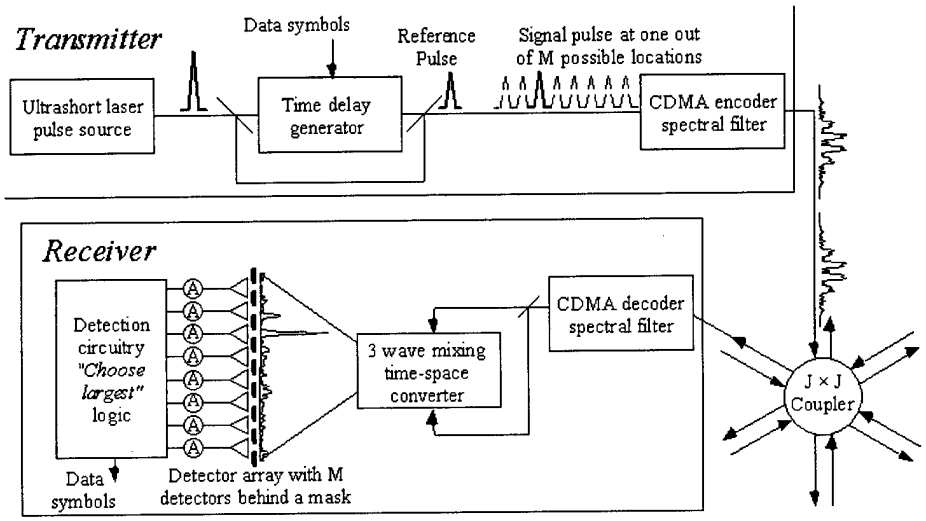

Fig. 5. System layout for hybrid PPM/CDMA privacy enhamvced communication network, consisting of transmitter, network star coupler, and receiver.

Many recent studies have investigated optical pulse position modulation (PPM) techniques to improve the performance of optical communication systems. However, analysis of such systems have not shown advantage of PPM over OOK for a fixed throughput and chip duration in an optical CDMA system. Some modified schemes, including overlapping PPM (OPPM) and bipolar PPM with spectral CDMA encoding, have been investigated to increase the bandwidth effciency. In the ULP-CDMA systems, however, the situation is diferent. Since a large bandwidth of ULP is a given, it is of importance to determine how to utilize the bandwidth effectively. New techniques for synthesis and detection of ultrashort waveforms developed at UCSD enables realization of such bandwidth-efficient PPM/ULP-CDMA systems. The hybrid

PPM/ULP-CDMA network system shown in Fig.5 has been investigated by our group for enhanced privacy communication applications. The all-optical multiplexer or synthesizer at the transmitter of an optical communication system, combines parallel optical channels modulated with electronic circuitry into an ultrahigh bandwidth fiber-optic channel (i.e., parallel-to-serial conversion) via a space-to-time transformation. At the receiver, a demultiplexer performs the inverse time-to-space transformation for electronic detection by a detector array (i.e., serial-to-parallel conversion). The information bits are encoded at the transmitter by varying the time (i.e., spatial coordinate of the modulators in the array) at which the pulse is transmitted. If we wish to encode b bits on each pulse, the transmitter will need to select one of M transmission slots (where $M=2^b$) for the data encoded pulse. After decoding the CDMA signal at the receiver, a time-to-space conversion takes place. The transformed signal has the form of a bright spot at one location, corresponding to the properly decoded signal, and random low intensity light from other users distributed elsewhere. A photo-detector array, placed behind a mask with narrow slits at locations corresponding to the time delays utilized in the PPM, detects the time-to-space mapped signal. The slits perform the required femtosecond scale time filtering. Decision circuitry at the receiver selects the largest signal from the detector array, extracting the transmitted data symbol. The 'choose largest' decision logic improves the bit error rate performance, as the decision is based on M statistical measurements.

B. 2 Ultrafast optical waveform detection and synthesis

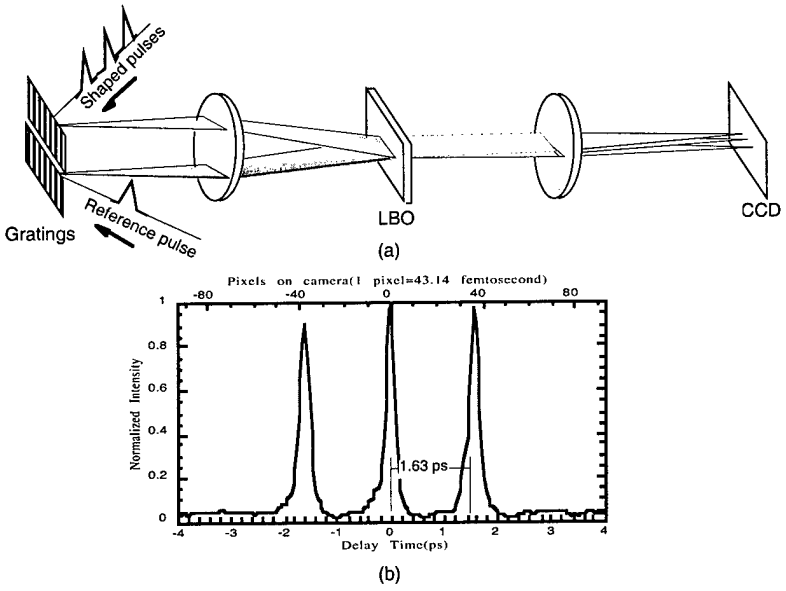

Fig. 6. (a) Femtosecond pulse imaging system based on nonlinear spectral domain 3-wave mixing in LBO crystal (b) Intensity profile measured from a shaped pulse that consists of three pulses separated by 1.63 picoseconds.

The ultrafast waveform imager performs serial-to-parallel demultiplexing of the shaped pulse train into parallel spatial channels for electronic detection. Our pulse image converter (PIC) system is capable of real-time conversion of a femtosecond pulse sequence into its spatial image. The approach employs spectral domain nonlinear 3-wave mixing in a LiB_3O_5 (LBO) crystal, where the spectral decomposition waves (SDW) of a shaped femtosecond pulse are mixed with those of a transform limited pulse to generate a quasi-monochromatic second harmonic field (see Fig. 6a). Through this nonlinear process, the temporal frequency content of the shaped pulse is directly encoded onto the spatial frequency content of the second harmonic field, producing a spatial image of the temporal shaped pulse after a spatial Fourier transform. The two incident beams arrive in opposite directions, in order to obtain the necessary spectrum inversion of the

corresponding SDW. The beams are vertically displaced to satisfy the non-collinear phase matching condition. These two beams are introduced into a LBO nonlinear crystal, generating a second harmonic field that propagates in a bisector direction that is parallel to the optical axis of the system. A second lens is used to perform a spatial Fourier transform of the second harmonic quasi-monochromatic field, producing an image that is detected by a CCD camera. In our experiments, we use a phase grating as a spectral filter in a standard pulse-shaping device. This grating produces three equal amplitude pulses separated by a distance 1.63 psec. The resultant shaped pulse image obtained with our PIC demultiplexer consists of 3 pulses spatially separated by a distance equivalent to 1.63 picoseconds (see Fig. 6b). The measurement results are found to be in excellent agreement with the calculated pulse shape obtained for the sinusoidal phase grating.

The ultrafast pulse synthesizer performs parallel-to-serial multiplexing of a parallel spatial image into a serial shaped pulse train with femtosecond response time and high conversion efficiency. Our CSN arrangement consists of a frequency-up conversion process followed by a frequency-down conversion process satisfying the type-II non-collinear phase matching condition. The non-linear wave mixing in our experiment takes place in the Fourier domain of the temporal and spatial channels (see Fig. 7). The first nonlinear process of the cascade mixes the SDW field U_1 of an input ultrashort pulse denoted by $p(t)$ and the spatial FT field U_2 of a quasi-monochromatic wave modulated spatially by a one-dimensional image denoted by m (x). The ordinary and extraordinary polarized fields U_1 and U_2, respectively, generate the intermediate up-converted SDW $U_{int} \sim \chi^{(2)} U_1 U_2$, polarized in the extraordinary direction. The second nonlinear process of the cascade mixes the intermediate SDW U_{int} and field U_3, the spatial FT of a narrow slit r(x) =δ(x). The narrow slit in the second spatial channel is illuminated by the same quasi-monochromatic source as U_2, and is co-propagating with U_2 after a polarizing beam splitter (see Fig. 7). The ordinary polarized field U_3 interacts with the extraordinary polarized SDW U_{int}, generating the output SDW $U_4 \sim (\chi^{(2)})^2 U_1 U_2 U_3^*$, which is equivalent to a four-wave mixing process. Thus, the femtosecond rate spatial-temporal processing has generated the SDW of the output temporal optical waveform. The SDW U_4 is recombined in the optical setup by a second FT lens and grating diffraction to yield the output temporal signal. This synthesized waveform is a convolution of the input ultrashort pulse $p(t)$ with the space domain image $m(x)$, whose spatial dependence has been converted to temporal dependence in the spatial-temporal processor. When the duration of the ultrashort pulse is much shorter than the feature size of the temporally mapped mask, then output temporal waveform is directly proportional to the information in the mask.

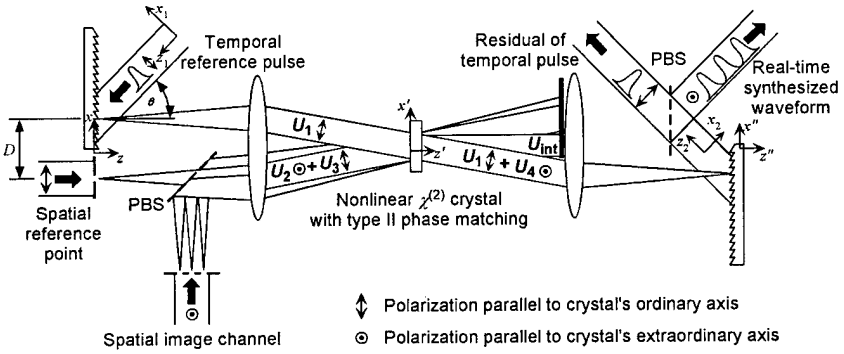

Fig. 7 Experimental setup of the spatial-temporal processor. The CSN enables time-space information exchange via a four-wave mixing process.

We demonstrate experimentally the CSN spatial-temporal wave mixing using ultrashort pulses of 100 fsec duration at a center wavelength of 800 nm with energy level of 1 mJ per pulse (generated from a Ti: Sapphire ultrashort pulse oscillator combined with a regenerative

amplifier) with a 2-mm thick BBO crystal. In our first spatial-temporal information transfer experiment, we used a mask containing a sequence of narrow slits spaced 0.8 mm apart. To achieve high light throughput, the illuminating beam was focused into the slits with a cylindrical lenslet array. The shaped waveform, consisting of a sequence of pulses, was observed with a real-time PIC technique (see Fig. 8). As predicted, the synthesized waveform consists of a sequence of pulses separated by ~1.3 psec (mapping spatial separation of 0.8 mm to time). Selectively blocking some of the slits resulted in a matching temporal waveform, confirming our ability to perform single shot temporal waveform synthesis in real-time from a spatial channel. These results were generated under maximal conversion efficiency, where fundamental wave depletion was observed. Therefore, by blocking some of the slits, more photons are upconverted by the spatial waves of the remaining open slits, leading to an amplitude distribution change in the pulse sequences of Fig. 8. No evidence of crosstalk between the channels was detected.

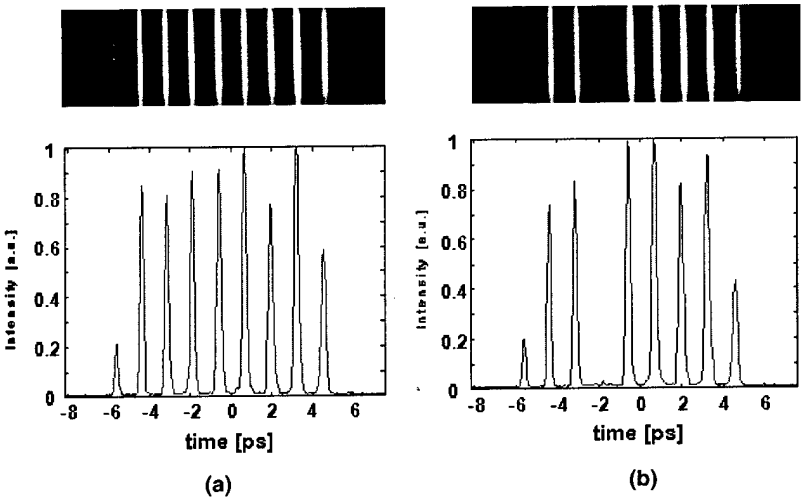

Fig. 8. Synthesized temporal waveform generated by a spatial information mask consisting of a sequence of equally spaced point sources. (a) All point sources are illuminated by quasi-monochromatic light. (b) One point source blocked.

Relative to other spatial-temporal processing techniques, our nonlinear wave mixing approaches to spatio-temporal processing provide femtosecond rate processing due to the fast bound electron nonlinearity and high efficiency on account of a relatively large $\chi^{(2)}$ coefficient in bulk crystals. The spatial-temporal process that we have demonstrated generate output spatial and temporal waveforms that can be changed in real time. Since the technique realizes a general wave mixing process of temporal and spatial information-carrying waves, the setup may be converted to provide the convolution or correlation signal between spatial and temporal channels, with the output in either the temporal or the spatial domain. Thus, this spatial-temporal process can be considered a fundamental system for performing ultrafast signal processing on optical waveforms in the time and space domain.

B. 3 Experimental PPM/CDMA system

We conducted preliminary experiments with the ULP-CDMA communication format, using our time/space converter, where each user will encode his transmitted pulse with a unique spectral filter. The most common system consists of two spatial Fourier transforms in cascade with diffraction gratings at the input and output plane. After the first spatial Fourier transform, at the spectral plane, the pulse's frequency components are linearly dispersed. CDMA encoding of ultrashort pulses can be performed by placing a pseudo-random mask in the spectral plane. The encoding mask divides the spectrum into narrow frequency bands, where each band has a value

of either +1 or –1, produced by an etched π phase delay. The encoded pulse that is transmitted onto a shared fiber resembles a noise burst, with its duration inversely proportional to the width of the frequency bands utilized in the mask.

The pulse imager at the receiver requires a reference pulse for converting the temporal signal to the space domain. As femtosecond scale time synchronization between transmitter and receiver is unfeasible, we consider transmitting the reference pulse along with the data encoded pulse[54]. Therefore, the information is encoded by the time difference between the two transmitted pulses. After the receiver's decoding filter, the two ultrashort pulses, with added pseudo-random background noise from other communicating members, perform the pulse imaging. This method eliminates laser pulse jitter from effecting the transmission, as the same seed pulse is used to generate the two transmitted pulses. Experimental results of PPM/CDMA modulation recovered data are shown in Fig. 9, where pulse images of three different time slots were chosen at the transmitter, and recovered faithfully at the receiver. Fig. 10 shows the received interference signal from an unmatched encoding/decoding CDMA pair, generating a low intensity signal distributed over a wide region. These experiments shows that the CDMA encoded data can be reconstructed by a legitimate code holder, thus providing enhanced privacy of the optical network system.

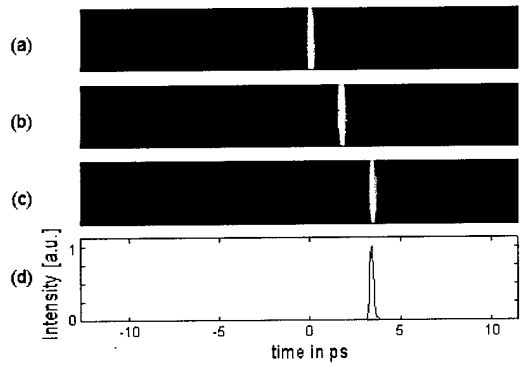

Fig. 9. Experimental results of recovered data from three different time slots using PPM/CDMA.

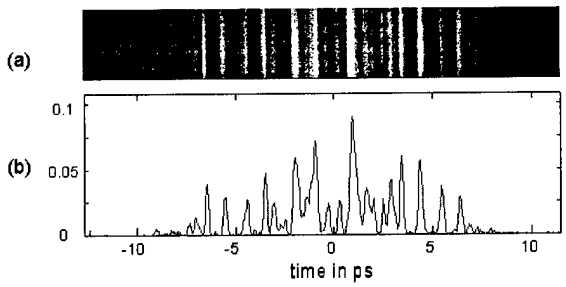

Fig. 10. (a) Experimental results of received interference from an unmatched transmitter using PPM/CDMA. The photo was enhanced for better visualization. (b) Signal values from unenhanced image.

In a network environment, many users transmit similarly encoded pulses, but with different codes. At the receiver, a second pulse shaping apparatus applies a second code to the received signal, which is a combination of all of the waveforms transmitted on the fiber. The pulse shaper at the receiver serves as a decoder, matching to only one of the waveforms transmitted on the fiber. Two communicating users employ the same code in the encoder and the

decoder, causing the encoded pulses to despread as the net resultant filter is unity for each frequency band (matched all-pass filters). When the codes of the transmitter and receiver do not match, as is the case for received signals from other users, the signal remains in the format of a time-spread pseudo-random noise burst. The high peak power despread signal is detected over the low background pseudo-random noise by a non-linear threshholder. In the following we describe the PPM/UPL-CDMA performance analysis in a multi-user environment.

5. Personnel Supported

Y. Fainman, PI, Professor

B. Slutsky, Research Assistant

D. Marom, Research Assistant

D. Panasenko, Research Assistant

W. Nakagawa, Research Assistant

K. Oba, Research Assistant

6. Publications

D. Marom, P. C. Sun, Y. Fainman, "Analysis of spatio/temporal converters for all-optical communication links," submitted to Appl. Opt.

B. Slutsky, R. Rao, P. C. Sun, L. Tancevski, and Y. Fainman, *Defense Frontier Analysis of Quantum Cryptographic Systems*, Appl. Opt. (submitted).

B. Slutsky, R. Rao, P.-C. Sun, Y. Fainman, *Security of quantum cryptography against individual attacks*, Phys. Rev. A (submitted).

B. Slutsky, P.C.Sun, Y.Mazurenko, R.Rao, and Y.Fainman, "Effect of channel imperfection on the secrecy capacity of a quantum cryptographic system," *J. of Modern Optics*, 44, No. 5, 953-961, 1997.

P. C. Sun, Y. Mazurenko, Y. Fainman, "Femtosecond pulse imaging: ultrafast optical oscilloscope," *JOSA A*, 14, 1159-1169, 1997

P. C. Sun, Y. Mazurenko, Y. Fainman," Real-time 1-D Coherent Imaging Through Single-mode Fibers by Space-Time Conversion Processors," *Opt. Lett.*, 22, 1861-1863, 1997.

B. Slutsky, R. Rao, P. C. Sun, L. Tancevski, and Y. Fainman, Defense Frontier Analysis of Quantum Cryptographic Systems, *Appl. Opt.*, 37, 2869-2878, 1998.

B. Slutsky, R. Rao, P.-C. Sun, Y. Fainman, Security of quantum cryptography against individual attacks, *Phys. Rev. A*, 57, 2383-2398, 1998.

D. Marom, P. C. Sun, Y. Fainman, "Analysis of spatio/temporal converters for all-optical communication links," *Appl. Opt.*, 37, 2858-2868, 1998.

K. Oba, P. C. Sun, and Y. Fainman, "Nonvolatile photorefractive spectral holography," *Opt. Lett.*, 23, 915-917, 1998.

Y. Mazurenko and Y. Fainman, "Cross talk of wavelength-multiplexed quasi-infinite holograms," *Opt. Lett.*, 23, 963-965, 1998.

Oba, P. C. Sun, Y. Mazurenko, and Y. Fainman, "Femtosecond single-shot correlation system: a time domain approach," *Applied Optics*, Vol. 38, no. 17, pp3810-3817, 1999

D. M. Marom, D. Panasenko, P. C. Sun, and Y. Fainman, " Spatial-temporal wave mixing for space-time conversion," *Opt. Lett.* **24**, 563-565(1999)

P. C. Sun, K. Oba, Y. Mazurenko, and Y. Fainman , "Space-time processing with photorefractive volume holography," *Proceedings of the IEEE*, vol.87, no.12, 2086-97, 1999 (invited paper)

D. M. Marom, D. Panasenko, R. Rokitski, P.-C. Sun, and Y. Fainman, "Instantaneous processing of ultrafast waveforms by wave mixing spectrally decomposed waves," special issue on Optics in 1999, *Optics and Photonics News*, 10, no. 12, 41-42, 1999

Mazurenko, Yu.T., Putilin, S.E., Belyaev, A.G., Spiro, A.G., and Y. Fainman, "Ultrafast transformation of a space-time signal into an image," Optika i Spektroskopiya, vol.87, no.1, 89-93, July 1999.

D. M. Marom, D. Panasenko, R. Rokitski, P.-C. Sun, and Y. Fainman, "Time reversal of ultrafast waveforms by wave mixing spectrally decomposed waves," *Opt. Lett* ., Vol. 25, No. 2, pp. 132-134, 2000.

W. Nakagawa, R. Tyan, P. C. Sun, Y. Fainman, "Near-field localization of ultrashort optical pulses in transverse 1-D periodic nanostructures," Optics Express, **7**, No. 3, pp. 123-128, 2000

P. C. Sun, Y. Mazurenko, and Y. Fainman , "Space-time processing with photorefractive volume holography using femtosecond laser pulses," Ch. 15 in book Photorefractive: Materials Properties and Applications, eds. F. T. S. Yu and S. Yin, Academic Press, pp. 485-518, 2000.

Y. Fainman, P. C. Sun, Y. Mazurenko, D. Marom, and K. Oba, " Nonlinear spatio-temporal processing with femtosecond laser pulses," NATO Science Series- 3/75 on "Unconventional Optical Elements for Information Storage, Processing, and Communication", ed. E. Marom, N. A. Vianos, A. A. Friesem, and J. W. Goodman, Kluwer academic publishers, Netherlands, pp. 163-171, 2000.

D. Marom, D. Panasenko, P. C. Sun, Y. Fainman, "Femtosecond rate space-to-time conversion," J. Opt. Soc. Am.: B, 17, 1759-73, 2000

D. Marom, D. Panasenko, R. Rokitski, P. C. Sun, Y. Mazurenko, and Y. Fainman, Reply to "Comment on 'Time reversal of ultrafast waveforms by wave mixing spectrally decomposed waves," Optics Letters, 25, 1209, 2000

D. Marom, D. Panasenko, P. C. Sun, Y. Fainman, "Linear and Nonlinear Operation of a Time-to-Space Processor," J. Opt. Soc. Am.: A, 18, 448-458, 2001

W. Nakagawa, R. Tyan, P. C. Sun, Y. Fainman, "Ultrashort Optical Pulse Propagation in Periodic Diffractive Structures using Rigorous Coupled-Wave Analysis," J. Opt. Soc. Am.:A, 18, pp. 1072-1081, 2001

7. Interactions/transitions

a. Meetings, Conferences, Seminars, Proceedings

B. Slutsky, R. Rao, Y. Fainman, " Security theorems in quantum cryptography," submitted to Proc. SPIE on Computer and Network Security Conference, Dallas, Texas, November 1997.

L. Tancevski, B. Slutsky, R. Rao, Y. Fainman, " Evaluation of the cost of error correction protocol in quantum cryptographic transmission," submitted to Proc. SPIE on Computer and Network Security Conference, Dallas, Texas, November 1997.

D. Marom, P. C. Sun, Y. Fainman, "Communication with ultrashort pulses and parallel-to-serial and serial-to-parallel converters," Proc. IEEE/LEOS, to be presented at the 10-th Annual Meeting of IEEE/LEOS, 1997..

Y. Fainman, "Optical interconnect systems for communications and computing," Proc. IEEE/LEOS, to be presented at the 10-th Annual Meeting of IEEE/LEOS, 1997 (invited).

B. Slutsky, R. Rao, L. Tancevski, P. C. Sun, Y. Fainman, "Quantum Cryptography: Defending against individual eavesdropping," presented at the SPIE Quantum Computing Conference, April 13-17, Orlando, Florida, 1998 (**Invited**).

Y. Fainman, "Space-time Information Processing with femtosecond Laser Pulses," presented at the International conferencxe on Optics in Computing, June 17-20, 1998, Brugge, Belgium; Proc. SPIE, 3490, 258-261, 1998 (**Invited**).

D. Marom, K. Oba, P. C. Sun, Y. Mazurenko, and Y. Fainman, "Spatio-temporal Conversion, Storage, and Processing using Femtosecond Optical Pulses," presented at the SPIE 43-rd Annual Meeting, July 1998, San Diego, California; Proc. SPIE, 3470, 64-76, 1998 Proceedings of the SPIE - The International Society for Optical Engineering, 1998, vol.3470:64-76 (**Invited**).

K. Oba, X. Zhang, P. C. Sun, Y. Mazurenko and Y. Fainman, "Single shot femtosecond/picosecond autocorrelator using tilted pulse front," presented at the SPIE 43-rd Annual Meeting, July 1998, San Diego, California; Proc. SPIE, 3466, 1998.

Y. Fainman and P. C. Sun, "Spatio-Temporal storage and retrieval with femtosecond optical pulses,"1998 International Photonics Conference, December 15-18, 1998, National Taiwan University, Taipei, Taiwan (**Invited**)

D. M. Marom, P.-C. Sun, and Y. Fainman, "Analysis of time-to-space converter," OSA Annual Meeting, Baltimore, MD, Oct. 98

Y. Fainman, "Nonlinear spatio-temporal processing for coherent optical communications," presented at the 1998 OSA Annual Meeting, October 4-9, 1998, Baltimore Maryland (**Invited**).

D. M. Marom, L. B. Milstein, and Y. Fainman, "Hybrid optical code division multiple access/pulse position modulation technique with self-referencing," OSA Annual Meeting, Baltimore, MD, Oct. 98.

D. M. Marom, D. Panasenko, P.-C. Sun, and Y. Fainman, "Real-time spatial-temporal signal processing by wave-mixing with cascaded second-order nonlinearities," presented at the OSA topical meeting on Optics for Computing, Snowmass, CO, April 1999.

D. M. Marom, D. Panasenko, P.-C. Sun, and Y. Fainman, "Spatial-temporal pulse waveform synthesis by wave-mixing with cascaded second-order nonlinearities," presented in Conference on Lasers and Electro-optics 1999 (CLEO'99), Baltimore, MD, May 1999.

K.Oba, X. Zhang, P. C. Sun, Y. T. Mazurenko, and Y. Fainman, "Single shot femtosecond/picosecond range autocorrelator using tilted pulse front" presented at the SPIE 43-rd Annual Meeting, July 1998, San Diego, California; also Proc. SPIE, 3466, pp. 185-195, 1998

Y. Fainman, P. C. Sun, Y. Mazurenko, D. Marom, and K. Oba, " Nonlinear spatio-temporal processing with femtosecond laser pulses," presented at the NATO Workshop on " Unconventional Optical Elements for Information Storage, Processing, and Communication", Kiryat Anavim, Israel, October 19-22, 1999. (**Invited**)

Y. Fainman, D. Marom, K. Oba, D. Panasenko, Y. Mazurenko, and P. C. Sun, "Nonlinear space-time information processing," presented at the Euro-American Workshop on Optoelectronic Information Processing, Colmar, France, May 31-June2, 1999; also appeared in the Critical review of SPIE, Optoelectronic Information Processing, B. Javidy and P. Refregier, ed., pp. 41-60, 1999. (**Invited**)

M. Marom, D. Panasenko, R. Rokitski, P.-C. Sun, and Y. Fainman, "Instantaneous time reversal of complex amplitude ultrafast waveforms," Proc. of LEOS'99 Annual Meeting, 1999 IEEE Lasers and Electro-Optics Society 1999 Annual Meeting

Y. Fainman, D. M. Marom, K. Oba, D. Panasenko, Y. T. Mazurenko, and P. C. Sun, "Nonlinear Spatio-temporal Processing," Proc. of LEOS'99 Annual Meeting, 1999 IEEE Lasers and Electro-Optics Society 1999 Annual Meeting (**invited**).

Y. Fainman, "Nonlinear Spatio-temporal Processing," Seminar at the School of Optics/CREOL, University of Central Florida, March 9-10, 2000.

Y. Fainman, D. Marom, D. Panasenko, R. Rokitski, K. Oba, Y. Mazurenko, and P. C. Sun, "Optical conversion between space and time parallelism," presented at the *Optics in Computing 2000*, Quebec City, Canada, June 18-23, 2000, *SPIE Conference Proceedings*, Vol 4089, p. 1028, 2000 (**Invited**)

D.M. Marom, K.S. Kim, L.B. Milstein, Y. Fainman, "Hybrid pulse position Modulation/ultrashort light pulse code division multiple access for data networking,"" *Optics in Computing 2000*, Quebec City, Canada, June 18-23, 2000, *SPIE Conference Proceedings*, Vol 4089, pp. 479-484, 2000.

Y. Fainman, "Nonlinear mixing of femtosecond laser pulses for communication and informationprocessing," presented at the Laser Optics 2000, St.-Petersburg, Russia, June 2000 (**Invited**)

K. Oba, P. C. Sun, Y. T. Mazurenko, Y. Fainman, "Femtosecond optics for data storage and detection," presented at the SPIE's 45-th Annual Meeting, paper #4110-33, July 2000 (**Invited**)

P. C. Sun, D. M. Marom, D. Panasenko, R. Rokitskii,P. C. Lin, Y. T. Mazurenko, and Y. Fainman, "Nonlinear space-time information processing," presented at the SPIE's 45-th Annual Meeting, paper #4113-01, July 2000 (**Keynote Address**)

Y. Fainman,"Nonlinear femtosecond informationprocessing systems," to be presented at the 2000 OSA/ILS XVI Annual Meeting, Providence, Rhode Island, 2000 (**Invited**)

L. B. Milstein, Y. Fainman, D. Marom, K. Kim, "Optical CDMA for Internet Operation at Terabit Rates," presented at the 2000 Second Annual International Symposium on Advanced Radio Technologies, September 6-8, 2000 (**Invited**)

Y. Fainman, D. Marom, D. Panasenko, Y. Mazurenko, and P. C. Sun, "Superfast information processing with femtosecond laser pulses," to be presented at the International Optical Congress "Optics - XXI Century", St. Petersburg, October 16-20, 2000 (**Invited**)

Y. Fainman, "Ultrafast optics for communications and computing," to be presented at the the IEEE/LEOS 2000 Annual Meeting, November 13-16, 2000 (**Invited**)

b. Consultative and advisory functions

Y. Fainman "Real-time optical analog-to-digital (ROAD) converters," presented at the DARPA Workshop on A/D Converter Technology, Arlington, October 1997.

Y. Fainman, " Optics in computing and communications," presentation and participation on the pannel "Potential Roles of Ultrafast Optics in Communications and Information Processing" at the 10-th Annual Meeting of IEEE/LEOS, 1997.

Y. Fainman, P. C. Sun, Y. Mazurenko, K. Oba, D. Marom, " Storage formats for ultrahigh speed communication and processing, presented at the AFOSR Workshop on Applications of Spectral Hole Burning, March 8-11, Montana State University, Bozman, Montana, 1998.

Y. Fainman, P. C. Sun, Y. Mazurenko, K. Oba, D. Marom, "Nonlinear Spatio-temporal Wave Mixing and Applications", presented at the AFOSR Workshop on Applications of Spectral Hole Burning, March 8-10, Montana State University, Bozman, Montana, 1999

Y. Fainman, P. Shames, "Single and Multi-beam Steering and LaserCom using Artificial Dielectrics", presented at the DARPA/ETO Workshop on Steering Agile Beams, March 24-25, Washington D. C. 1999.

Y. Fainman, "Dynamically Configurable Confocal Microscopy using the DMD Engine," presented at the 1999 DARPA/ETO MEMS Principal Investigators' Meeting, January 13-15, Baton Rouge, Louisiana, 1999

Y. Fainman, "Artificial Dielectric Materials and Integration," presented at the Annual Review of the DARPA's Heterogeneous Optoelectronics Technology Center, May 13-14, 1999, Santa Fe, New Mexico

Y. Fainman, D. Marom, K. Oba, D. Panasenko, Y. Mazurenko, and P. C. Sun, "Nonlinear space-time information processing with femtosecond laser pulses," presented in the Department of Chemistry, ETH Zurich, Switzerland, June 4, 1999

Y. Fainman, "Artificial Dielectrics," presented at the workshop on Electronic, Photonic, Electro-Optic and Magneto-Optic Materials, Redstone Arsenal, October 6-7, 1999 (Invited Presentation)

Y. Fainman, "3-D Quantitative Imaging," Colloquium at the University of Arizona's Optical Science Center, November 18, 1999.

Y. Fainman, "Nonlinear Spatio-temporal Processing," Seminar at the School of Optics/CREOL, University of Central Florida, March 9-10, 2000.

Y. Fainman, "Nanophotonics for on-chip integration of WDM systems," DARPA

WDM Workshop, April 18-19, 2000 (Invited talk)

Y. Fainman,"Programmable meso-optics with resonant near-firld nonlinear nanostructures," AFOSR Program Review, May 25-26, 2000 (reporting talk)

Y. Fainman, "Artificial Dielectric Materials and Integration," DARPA's HOTC

Center Review, July 27-28, 2000. (reporting talk)

8. New discoveries:

None

9. Honors/Awards:

None